平成 17 年度後期代数学 D・代数学基礎講義 B

都築 暢夫

第 II 部　代数体の整数論

第 II 部では、代数体の整数論、中でも代数体の整数環が Dedekind 環になることを証明する。一般に代数体の整数環においては、素因数分解の一意性が成り立たない。しかし、イデアル分解に概念を拡張させると素イデアル分解の一意性が成り立つ。この事実を利用して、Riemann ζ 関数は、自然に代数体の Dedekind ζ 関数 (第 III 部) へ拡張される。

Contents

参考文献

Lang, S., Algebraic number theory, GTM 110, Springer-Verlag, 1986.
永田雅宜, 「可換環論」紀伊国屋数学叢書 1, 紀伊國屋書店, 1974.
Serre, J.P., Local fields, GTM 67, Springer-Verlag, 1979. (仏語版が元本)

1. 代数体とその整数環

1.1. **代数体の整数環.** 代数体とその整数環を導入する。

定義 1.

有理数体 $\mathbb{Q}$ の有限次拡大体を**代数体**という。

定義 2.

K を代数体とする。K の元で有理整数環 $\mathbb{Z}$ 上整な元全体の集合 $\mathcal{O}_K$ のことを K の**整数環**という。

ここで、

定義 3.

(1) S/R が整域の拡大とは、S が R 代数として $R \subset S$ となることをいう。
(2) S/R を整域の拡大とする。S の元 α が R 上**整**とは、0 でない R 係数単多項式 $f(x) \in R[x]$ が存在して、$f(\alpha) = 0$ となることをいう。
(3) 整域 R が**整閉整域** (**正規整域**ともいう) とは、R の商体の元で R 上整な元はすべて R に属するものをいう。

である。よく知られている事実として、

$$\text{Euclid 整域 (E.D.)} \Rightarrow \text{単項イデアル整域 (P.I.D.)} \Rightarrow \text{一意分解整域 (U.F.D.)} \Rightarrow \text{整閉整域}$$

が成り立つ。

$\mathcal{O}_K$ が、環になることは後で証明する。体の中だから、$\mathcal{O}_K$ は必然的に整域になる。

定義 4.

R が **Dedekind 環**とは、Noether 整閉整域で、(0) でない任意の素イデアルが極大イデアルであるものをいう。

定理 5.

代数体 K の整数環 $\mathcal{O}_K$ は Dedekind 環である。また、$K = \mathbb{Q}\mathcal{O}_K$ であり、$\mathcal{O}_K$ は $\mathbb{Z}$ 上の階数 $[K : \mathbb{Q}]$ の自由加群である。

$K = \mathbb{Q}\mathcal{O}_K$ の意味は、$\mathbb{Q}$ ベクトル空間として $\mathcal{O}_K$ は K を生成するということである。次節以降で必要な可換環論・体論を準備して、この定理を証明する。

1.2. 2 **次体の整数環.**

定義 6.

$\mathbb{Q}$ 上の 2 次拡大体を **2 次体**という。

定義 7.

整数 D が平方因子を持たないとは、$D \neq 0, 1$ かつ 2 以上の整数の 2 乗で割り切れないものをいう。

命題 8.

次の対応は全単射である。

$$\begin{array}{ccc} \{D \,|\, D \text{ は平方因子を持たない整数 }\} & \to & \{K \subset \mathbb{C} \,|\, K \text{ は 2 次体 }\} \\ D & \mapsto & \mathbb{Q}(\sqrt{D}) \end{array}$$

$D > 0$ のとき $\mathbb{Q}(\sqrt{D})$ を**実 2 次体**、$D < 0$ のとき $\mathbb{Q}(\sqrt{D})$ を**虚 2 次体**という。

定理 9.

D を平方因子を持たない整数とし、$K = \mathbb{Q}(\sqrt{D})$ とする。このとき、

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\dfrac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \end{cases}$$

が成り立つ。$\mathcal{O}_K$ は加法・乗法に関して閉じていて整域になる。特に、$\mathcal{O}_K$ は $\mathbb{Z}$ 上の階数 2 の自由加群である。

$\because$ 右辺の各元が $\mathbb{Z}$ 上整なのは明らか。$a + b\sqrt{D}\,(a, b \in \mathbb{Q})$ が $\mathbb{Z}$ 上整とする。下の Gauss の補題から、$a + b\sqrt{D}$ の $\mathbb{Q}$ 上の最小多項式 $p(x) = x^2 - 2ax + (a^2 - b^2 D)$ は、$\mathbb{Z}$ 係数の多項式である。したがって、$2a, a^2 - b^2 D$ はともに整数である。

$D \equiv 1 \pmod 4$ とする。a は整数または $1/2$ 足す整数となる。a が整数のときは、$b^2 D$ も整数で、D は平方因子を持たないから b も整数である。この場合、$a + b\sqrt{D} = (a - b) + 2b(1 + \sqrt{D})/2$ となり、これは右辺に含まれる。a が $1/2$ 足す整数のときは、$b^2 D$ は $1/4$ 足す整数でなければならない、$D \equiv 1 \pmod 4$ なので、b が $1/2$ 足す整数となる。よって、$a + b\sqrt{D} - (1 + \sqrt{D})/2$ が整数足す $\sqrt{D}$ の整数倍になり、$a + b\sqrt{D}$ は右辺に属する。

他の場合も同様にやればできるので、証明を略する。

特にの部分の証明：$D \equiv 1 \pmod 4$ とする。

$$\left(\frac{1+\sqrt{D}}{2}\right)^2 = (1 + D + 2\sqrt{D})/4 = \frac{1+\sqrt{D}}{2} + (D-1)/4$$

なので、1 と $\frac{1+\sqrt{D}}{2}$ が $\mathbb{Z}$ 上の基底になる。 □

定理 (Gauss の補題) 10.

1 次以上の整係数単多項式が整係数多項式として既約ならば、有理係数多項式として既約である。

2. 環論の復習

必要な環論を復習する。R を環 (このノートで環といえば可換環を意味する) とする。また、R の元 a, b に対して、

$$a \mid b \Leftrightarrow \exists c \in R \text{s.t.} \, b = ac$$

と定め、a が b を**割り切る**という。

2.1. 局所化.

定義 11.

R の部分集合 S が**積閉集合**とは、(i) $a, b \in S \Rightarrow ab \in S$ と (ii) $1 \in S, 0 \notin S$ が成り立つことをいう。

命題 12.

I を R のイデアルとするとき、$S = R \setminus I$ が R の積閉集合になるための必要かつ十分条件は I が R の素イデアルであることである。

定理 13.

R 代数 $S^{-1}R$ で、次の普遍性を満たすものが標準的同型を除いてただ一つ存在する。

普遍性 : 環準同型 $f : R \to A$ で、任意の $s \in S$ に対して $f(s)$ が A の単元となるものに対して、環準同型 $g : S^{-1}R \to A$ で、図式 $\begin{array}{ccc} R & \xrightarrow{f} & A \\ \downarrow & \nearrow g & \\ S^{-1}R & & \end{array}$ が可換になるものがただ一つ存在する。

$S^{-1}R$ は、$R \times S$ 上の同値関係

$$(a, s) \sim (b, t) \Leftrightarrow \exists u \in S \text{s.t.} \, u(at - bs) = 0$$

による商集合上に、自然な方法で加法と乗法を定めて構成される。

R が整域で、積閉集合 $R \setminus \{0\}$ で局所化すると R の商体になる。

命題 14.

S を R の積閉集合、$\iota : R \to R_{\mathfrak{p}}$ を自然な環準同型とする。R の素イデアル $\mathfrak{p}$ に対して、$\mathfrak{p} \cap S \neq \emptyset$ ならば $\iota(\mathfrak{p})S^{-1}R = S^{-1}R$ であり、$\mathfrak{p} \cap S = \emptyset$ ならば $\iota(\mathfrak{p})S^{-1}R$ は素イデアルである。さらに、これは、写像

$$\{S^{-1}R \text{の素イデアル}\} \to \{R \text{の素イデアル } \mathfrak{p} \text{ で } \mathfrak{p} \cap S = \emptyset\} \quad \mathfrak{q} \mapsto \iota^{-1}(\mathfrak{q})$$

の逆写像を与える。

$\because$ $\mathfrak{p}$ を R の素イデアルとする。$\mathfrak{p} \cap S \neq \emptyset$ ならば $\iota(\mathfrak{p})S^{-1}R = S^{-1}R$ は明らか。

$\mathfrak{p} \cap S = \emptyset$ とする。$\iota(\mathfrak{p})S^{-1}R = S^{-1}R$ とすると、$\sum a_i/s_i = 1$ となる。すなわち、ある $s \in S$ と $a \in \mathfrak{p}$ が存在して、$sa \in S \cap \mathfrak{p}$ となる。よって、$\iota(\mathfrak{p})S^{-1}R$ は真のイデアルである。

$\mathfrak{p}S^{-1}R$ が素イデアルになることを証明する。$(a/s)(b/S) \in \iota(\mathfrak{p})S^{-1}R (a, b \in R, s, r \in S)$ とする。ある $u \in S$ が存在して、$uab \in \mathfrak{p}$ となる。$\mathfrak{p}$ は素イデアルより、a または b が $\mathfrak{p}$ に属する。

$\iota^{-1}(\iota(\mathfrak{p})S^{-1}R) = \mathfrak{p}$ を示す。$a \in \iota^{-1}(\iota(\mathfrak{p})S^{-1}R)$ とする。$\iota(a) \in \iota(\mathfrak{p})S^{-1}R$ なので、ある $s \in S$ が存在して、$sa \in \mathfrak{p}$ となる。よって、$a \in \mathfrak{p}$ である。逆向きの包含関係は成り立つので、$\iota^{-1}(\iota(\mathfrak{p})S^{-1}R) = \mathfrak{p}$ である。

$\mathfrak{q}$ を $S^{-1}R$ の素イデアルとする。$\iota^{-1}(\mathfrak{q})S^{-1}R = \mathfrak{q}$ を証明する。$a/s \in \iota^{-1}(\mathfrak{q})S^{-1}R (a \in \iota^{-1}(\mathfrak{q}), s \in S)$ とする。$\iota(a) \in \mathfrak{q}$ なので、$a/s = \iota(s)^{-1}\iota(a) \in \mathfrak{q}$ である。逆向きの包含関係も同様に示せる。 □

$\mathfrak{p}$ を環 R の素イデアルとし、$S = R \setminus \mathfrak{p}$ とする。このとき、$S^{-1}R$ を R の素イデアル $\mathfrak{p}$ での局所化といい、$R_{\mathfrak{p}}$ と表す。$R_{\mathfrak{p}}$ は $\mathfrak{p}R_{\mathfrak{p}}$ を唯一の極大イデアルに持つ局所環である。

命題 15.

R を環、$\mathfrak{m}$ を R の極大イデアルとする。任意の正整数 i に対して、自然な写像 $R/\mathfrak{m}^i \to R_{\mathfrak{m}}/\mathfrak{m}^i R_{\mathfrak{m}}$ は同型になる。

∵ 任意の $s \notin \mathfrak{m}$ に対して、ある $t \notin \mathfrak{m}$ が存在して、$st-1 \in \mathfrak{m}^i$ となる。実際、$R/\mathfrak{m}$ は体だから、$st'-1 \in \mathfrak{m}$ となる t' が存在する。$st' = 1+y$ として、$st'(1-y+y^2-\cdots+(-1)^{i-1}y^{i-1}) = 1+(-1)^{i-1}y^i$ となり、$y^i \in \mathfrak{m}^i$ となる。

準同型定理より、自然な写像 $R \to R_{\mathfrak{m}}/\mathfrak{m}^i R_{\mathfrak{m}}$ が全射かつその核が $\mathfrak{m}^i$ であることを示せばよい。$R_{\mathfrak{m}}$ の元は $x/s\,(x \in R, s \notin \mathfrak{m}$ と表される。$st-1 \in \mathfrak{m}^i$ となる $t \notin \mathfrak{m}$ をとると、$x/s = (xt)/(st) \equiv xt \pmod{\mathfrak{m}^i R_{\mathfrak{m}}}$ となる。よって、自然な写像で $xt \in R$ が x/s に移る。

x が写像の核になるとすると、ある $s \notin \mathfrak{m}$ が存在して $sx \in \mathfrak{m}^i$ となる。$st-1 \in \mathfrak{m}^i$ となる t を掛けると、$x \in \mathfrak{m}^i$ が解る。 □

命題 16.

P.I.D.、U.F.D.、整閉整域の局所化はそれぞれ、P.I.D.、U.F.D.、整閉整域である。

2.2. **中山の補題と中国式剰余定理.** この二つの命題は、その主張自体は容易に理解できるものであるが、環論を展開する上で重要な手段となる。

命題 (中山の補題) 17.

I をすべての極大イデアルに含まれる R のイデアルとする。M を有限生成 R 加群、N をその部分 R 加群とする。もし、$M = N + IM$ ならば、$M = N$ である。

∵ M/N を考えることにより、$N = 0$ としてよい。$x_1, \cdots, x_n$ を M の生成元とする。このとき、$a_{ij} \in I\,(1 \le i, j \le n)$ が存在して

$$x_i = a_{1i}x_1 + a_{2i}x_2 + \cdots + a_{ni}x_n$$

となる。I に関する仮定から、n 次正方行列 $1_n - (a_{ij})$ (1_n は単位行列) の行列式は R の単元となる。よって、$x_i = 0\,(\forall i)$ となる。したがって、$M = 0$ である。 □

命題 (中国式剰余定理) 18.

$I_1, I_2, \cdots, I_n$ を R のイデアルで、任意の $i \neq j$ に対して $I_i + I_j = R$ となるとする。このとき、$I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$ であり、自然な準同型

$$R/I_1 I_2 \cdots I_n \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

は同型である。

2.3. **Noether 環.** Noether 環について必要な知識をまとめておく。

命題-定義 19.

以下の同値な条件を満たす可換環 R を **Noether 環**という。

(i) $I_0 \subset I_1 \subset \cdots$ を R のイデアルの無限増大列とする。このとき、ある n が存在して、$I_n = I_{n+1} = I_{n+2} = \cdots$ となる。

(ii) Φ を R のイデアルのなす空でない集合とする。このとき、Φ には包含関係に関して極大元が存在する。

(iii) R の任意のイデアルは有限生成である。

体や P.I.D. は Noether 環である。

定理 20.

R を Noether 環とする。このとき、R 係数の多項式環、R のイデアル I による剰余環 R/I、R の積閉集合 S による局所化 $S^{-1}R$ は Noether 環である。

系 21.

R を Noether 環とするとき、R 上の有限型代数 ($R[x_1, \cdots, x_n]/I$ と表される環) は Noether 環である。特に、R 代数 A が R 加群として有限生成ならば、A は Noether 環である。

2 次体の整数環は $\mathbb{Z}$ 加群として階数 2 の自由加群なので、Noether 環である。

命題 22.

M を R 加群、N を M の R 部分加群とする。

(1) N と M/N が有限生成 R 加群ならば M は有限生成 R 加群である。
(2) M が有限生成 R 加群ならば M/N は有限生成 R 加群である。
(3) R を Noether 環とする。M が有限生成 R 加群ならば N は有限生成 R 加群である。

2.4. **単因子論.** 次の定理が、単因子論の主定理である。

定理 23.

R を P.I.D. とする。R 係数 $m \times n$ 行列 A に対して、可逆な R 係数 m 次正方行列 P、可逆な R 係数 n 次正方行列 Q、ある $\lambda_1, \cdots, \lambda_s \in R \setminus \{0\}\,(s \leq \min\{m, n\})$ が存在して、

$$P^{-1}AQ = \begin{pmatrix} \lambda_1 & & & & & & \\ & \lambda_2 & & & & & \\ & & \ddots & & & & \\ & & & \lambda_s & & & \\ & & & & 0 & & \\ & & & & & \ddots & \end{pmatrix} \qquad \text{ただし、} \lambda_1 \,|\, \lambda_2 \,|\, \cdots \,|\, \lambda_s$$

とできる。$\lambda_1, \cdots, \lambda_s$ を A の単因子といい、R のイデアル列 $(\lambda_1) \supset (\lambda_2) \supset \cdots \supset (\lambda_s)$ として一意的である。言い換えると、単因子は単元倍を除いて一意的である。
特に、R が Euclid 整域のとき、P と Q は行列の初等操作

(i) ある行 (列) を単数倍する。
(ii) 2 つの行 (列) を入れ替える。
(iii) ある行 (列) に、他の行 (列) に R の元倍したものを加える。

の繰り返しに対応する可逆行列になる。

例. $R = \mathbb{Z}$ とする。$A = \begin{pmatrix} 13 & 5 & 32 & 77 \\ 12 & 6 & 30 & 72 \\ 24 & -32 & 48 & 112 \end{pmatrix}$ のとき、初等操作を繰り返すと

$$\begin{pmatrix} 13 & 5 & 32 & 77 \\ 12 & 6 & 30 & 72 \\ 24 & -32 & 48 & 112 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 & 5 \\ 12 & 6 & 30 & 72 \\ 24 & -32 & 48 & 112 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 & 5 \\ 0 & 18 & 6 & 12 \\ 0 & -44 & -12 & 32 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & -1 & 2 & 5 \\ 0 & 18 & 6 & 12 \\ 0 & 10 & 6 & 68 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 & 5 \\ 0 & -2 & -6 & -124 \\ 0 & 10 & 6 & 68 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & -1 & 2 & 5 \\ 0 & -2 & -6 & -124 \\ 0 & 0 & -24 & -552 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 24 & 0 \end{pmatrix}$$

となるので、A の単因子は $1, 2, 24$ である。

系 24.

R を P.I.D.、M を有限生成 R 加群とする。このとき、非負整数 r と $\lambda_1, \lambda_2, \cdots, \lambda_s \in R \setminus (\{0\} \cup R^\times)$ で $\lambda_1 \,|\, \lambda_2 \,|\, \cdots \,|\, \lambda_s$ を満たすものが存在して、

$$M \cong R^{\oplus r} \oplus R/(\lambda_1) \oplus \cdots \oplus R/(\lambda_s)$$

となる。ただし、$R^{\oplus r}$ で階数 r の自由加群を表す。

$\because$ M は有限生成だから、ある正の整数 m と全射 R 準同型 $\varphi : R^{\oplus m} \to M$ が存在する。R は Noether 環だから φ の核 $\ker\varphi$ も有限生成である。よって、ある正の整数 n と全射 R 準同型 $\psi : R^{\oplus n} \to \ker\varphi$ が存在する。$f : R^{\oplus n} \to R^{\oplus m}$ を ψ と包含写像 $\ker\varphi \subset R^{\oplus m}$ の合成写像とする。R 係数 $m \times n$ 次行列 A を、$R^{\oplus m}$ と $R^{\oplus n}$ の標準的基底 $(u_1, \cdots, u_m)$ と $(v_1, \cdots, v_n)$ に関する R 準同型 f の表現行列 $f(v_1, \cdots, v_n) = (u_1, \cdots, u_m)A$ とする。単因子論から、ある可逆行列 P と Q、ある R の元の列 $\lambda'_1 \,|\, \cdots \,|\, \lambda'_s$ が存在して、$P^{-1}AQ = \begin{pmatrix} \lambda'_1 & & \\ & \lambda'_2 & \\ & & \ddots \end{pmatrix}$ とできる。$R^{\oplus m}$ と $R^{\oplus n}$ の基底を $(u_1, \cdots, u_m)P$ と $(v_1, \cdots, v_n)Q$ と取り直すと、f は対角的な行列 $P^{-1}AQ$ で表されるので、

$$M \cong R^{\oplus m-s} \oplus R/(\lambda'_1) \oplus \cdots \oplus R/(\lambda'_s)$$

となる。λ' が単元のとき、$R/(\lambda') = 0$ となるので、単元となる $\lambda'_1 \cdots$ を除くと定理が証明できた。 □

$\mathbb{Z}$ 加群はアーベル群より、$R = \mathbb{Z}$ のとき、有限生成アーベル群の基本定理という。

例. $\mathbb{Z}^{\oplus 4}$ の部分群 K を $(13, 5, 32, 77), (12, 6, 30, 72), (24, -32, 48, 112)$ で生成される $\mathbb{Z}^{\oplus 4}$ の部分群を K とし、$M = \mathbb{Z}^{\oplus 4}/K$ とする。このとき、M は上の例の行列 $A = \begin{pmatrix} 13 & 5 & 32 & 77 \\ 12 & 6 & 30 & 72 \\ 24 & -32 & 48 & 112 \end{pmatrix}$ で表現される準同型 $f : \mathbb{Z}^{\oplus 3} \to \mathbb{Z}^{\oplus 4}$ の余核になる。A の単因子は 1, 2, 24 より、

$$M \cong \mathbb{Z} \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(24)$$

となる。

命題 25.

R を P.I.D.、K を R の商体とする。V を有限次元 K ベクトル空間、Γ を V の有限生成部分 R 加群とする。このとき、Γ は自由 R 加群で、

$$\mathrm{rank}_R \Gamma \leq \dim_K V$$

が成り立つ。不等式の等号が成り立つための必要十分条件は、Γ が K 上 V を生成することである。

$\because$ Γ には捻れ元がないから、定理 24 より自由 R 加群になる。K が R の商体であるから、Γ の基底が K 上一次独立になることが解る。等号の必要十分性は明らか。 □

注. Γ の有限生成性をはずすと、上の命題は成り立たない。例えば、$R = \mathbb{Z}, V = \Gamma = \mathbb{Q}$ など。

命題 26.

K を体、μ を K の乗法群の有限部分群とする。このとき、μ は巡回群である。

$\because$ 有限生成アーベル群の基本定理から、

$$\mu \cong \mathbb{Z}/(n_1) \oplus Z/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_r) \quad 1 < n_1 \,|\, n_2 \,|\, \cdots \,|\, n_r$$

となる (有限群より、自由加群の部分はない)。よって、$x^{n_1} = 1$ となる μ の元は n_1^r 個ある。一方、K は体より、$x^{n_1} = 1$ の K の中での解は高々 n_1 個である。したがって、$r = 1$ となり、μ は巡回群である。 □

3. 体論の復習

必要な体論を復習する。

3.1. **非分離拡大.**

定義 27.

K を標数が 0 でない体とし、L/K を代数拡大とする。

(1) $\alpha \in L$ が K 上**純非分離的**とは、α の K 上の最小多項式 $p_{\alpha,K}(x)$ がただ一つの根しか持たないことをいう。

(2) L/K が**純非分離拡大**とは、L のすべての元が K 上純非分離的であることをいう。

命題 28.

K を標数が $p > 0$ の体とし、L/K を代数拡大とする。$\alpha \in L$ が K 上純非分離的ならば、ある非負整数 n が存在して、$\alpha^{p^n} \in K$ となる。さらに、f をこのような整数の中で最小の整数とすると、$p_{\alpha,K}(x) = x^{p^f} - \alpha^{p^f}$ となる。

命題 29.

K を標数が $p > 0$ の体とし、L/K を代数拡大とする。このとき、次は同値である。

(i) L/K は純非分離拡大である。

(ii) ある K 上の純非分離的な元 $\alpha_1, \cdots \in L$ (無限個でもよい) が存在して、$L = K(\alpha_1, \cdots)$ となる。

(iii) $\overline{K}$ を K の代数閉包とし、$\iota : K \to \overline{K}$ を埋め込みとすると、ι は L 上に一意的に延びる。

特に、L/K が有限次純非分離拡大ならばその次数は p のべきになる。

命題-定義 30.

K を標数が $p > 0$ の体とし、L/K を代数拡大とする。

(1) K_s を K 上分離的な L の元全体からなる集合とすると、L/K_s は純非分離拡大になる。K_s を K の L の中での**分離閉包**という。

(2) K_i を K 上純非分離的な L の元全体からなる集合とすると、L/K_i は分離拡大になる。K_i を K の L の中での**純非分離閉包**という。

(3) $L = K_s K_i$

(4) L/K が有限次拡大のとき、$[K_s : K] = [L : K_i]$ となる。

標数 0 では、代数拡大はいつでも分離拡大なので、純非分離部分はいつでも自明な拡大になる。

3.2. **ノルムとトレース.** L/K を有限次体拡大、L を K 上のベクトル空間とみなし、$e_1, e_2, \cdots, e_d\,(d = [L : K])$ を L の K 上の基底とする。$\alpha \in L$ に対して、K 線形写像 $l_\alpha : L \to L$ を $l_\alpha(v) = \alpha v$ で定め、その行列表示 A_α を

$$l_\alpha(e_1, e_2, \cdots, e_d) = (e_1, e_2, \cdots, e_d)A_\alpha$$

とする。写像

$$L \to \mathrm{Mat}(d, K) \quad \alpha \mapsto A_\alpha$$

を基底 $e_1, e_2, \cdots, e_d$ に関する L **の** K **上の表現**という。ただし、$\mathrm{Mat}(d, K)$ で K 上の d 次正方行列全体のなす環を表す。

次の補題は容易である。

補題 31.

(1) $A_{\alpha+\beta} = A_\alpha + A_\beta$
(2) $A_{\alpha\beta} = A_\alpha A_\beta$
(3) $a \in K$ に対して、$A_a = aE_d$ となる。ただし、E_d で d 次の単位行列を表す。
特に、L の K 上の表現は K 代数の環準同型である。

$e'_1, e'_2, \cdots, e'_d$ を L の K 上のもう一つの基底とする。このとき、d 次可逆行列 P が存在して、$(e'_1, e'_2, \cdots, e'_d) = (e_1, e_2, \cdots, e_d)P$ となる。基底 $e'_1, e'_2, \cdots, e'_d$ に関する $\alpha \in L$ の行列表示を A'_α で表すと、

$$l_\alpha(e'_1, e'_2, \cdots, e'_d) = l_\alpha(e_1, e_2, \cdots, e_d)P = (e_1, e_2, \cdots, e_d)A_\alpha P = (e_1, e_2, \cdots, e_d)P^{-1}A_\alpha P$$

となる。したがって、任意の $\alpha \in L$ に対して

$$A'_\alpha = P^{-1}A_\alpha P$$

である。

定義-命題 32.

(1) L/K を有限次体拡大とし、L の K 上の表現 $(\alpha \mapsto A_\alpha)$ を固定する。写像 $T_{L/K}$ と $N_{L/K}$ を

$$T_{L/K} : L \to K \quad \alpha \mapsto \mathrm{trace}(A_\alpha)$$
$$N_{L/K} : L \to K \quad \alpha \mapsto \det(A_\alpha)$$

と定めて、L の K 上の**トレース**と**ノルム**という。トレースとノルムは、L の K 上の基底の取り方によらない。
(2) $\alpha, \beta \in L$ に対して、次が成り立つ。

$$T_{L/K}(\alpha+\beta) = T_{L/K}(\alpha) + T_{L/K}(\beta)$$
$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$$

(3) $a \in K, \alpha \in L$ に対して、次が成り立つ。

$$T_{L/K}(a) = [L:K]a, \quad T_{L/K}(a\alpha) = aT_{L/K}(\alpha)$$
$$N_{L/K}(a) = a^{[L:K]}$$

定義-命題 33.

(1) L/K を有限次体拡大とし、L の K 上の表現 $(\alpha \mapsto A_\alpha)$ を固定する。$\alpha \in L$ の K 上の**特性多項式**を

$$\varphi_{\alpha,L/K}(x) = \det(xE_{[L:K]} - A_\alpha)$$

と定めると、$\varphi_{\alpha,L/K}(x)$ は L の K 上の基底の取り方によらない。特に、

$$\varphi_{\alpha,L/K}(x) = x^{[L:K]} - T_{L/K}(\alpha)x^{[L:K]-1} + \cdots + (-1)^{[L:K]}N_{L/K}(\alpha)$$

になる。
(2) $p_{\alpha,K}(x)$ を $\alpha \in L$ の K 上の最小多項式とすると

$$\varphi_{\alpha,L/K}(x) = p_{\alpha,K}(x)^{[L:K(\alpha)]}$$

となる。

$\because$ (1) は明らか。
(2) $K(\alpha)$ の K 上の基底を $u_1, \cdots, u_d$ とし、L の $K(\alpha)$ 上の基底を $v_1, \cdots, v_e$ とすると、L の K 上の基底として $u_1v_1, u_2v_1, \cdots, u_dv_e$ がとれる。A_α を α の $u_1, \cdots, u_d$ に関する表現行列、B_α を α の $u_1v_1, u_2v_1, \cdots, u_dv_e$ に関する表現行列とする。αu_i は $K(\alpha)$ の元なので、$\alpha u_i v_j$ は $K(\alpha)v_j$ に属する。よって、

$$B_\alpha = \begin{pmatrix} A_\alpha & & \\ & \ddots & \\ & & A_\alpha \end{pmatrix}$$

となる (成分を書いてない部分は 0 とする)。従って、命題が成り立つ。 □

命題 34.

L/K を有限次体拡大とし、M を L/K の中間体とするとき、次が成り立つ。

$$T_{L/K} = T_{M/K} \circ T_{L/M}$$
$$N_{L/K} = N_{M/K} \circ N_{L/M}$$

$\because$ $\alpha \in L$ に対して、$T_{L/K}(\alpha) = T_{M/K} \circ T_{L/M}(\alpha)$ と $N_{L/K}(\alpha) = N_{M/K} \circ N_{L/M}(\alpha)$ を証明する。

$L = M(\alpha)$ とする。M の K 上の基底を $u_1, \cdots, u_d$ とし、L の M 上の基底を $1, \alpha, \cdots, \alpha^{e-1}$ とすると、L の K 上の基底として $u_1, u_2, \cdots, u_1\alpha, \cdots, u_d\alpha^{e-1}$ がとれる。A_* を $*$ の $u_1, \cdots, u_d$ に関する表現行列、B_* を $*$ の $u_1, u_2, \cdots, u_1\alpha, \cdots, u_d\alpha^{e-1}$ に関する表現行列とする。

$$\alpha^e + a_1\alpha^{e-1} + \cdots + a_e = 0 \ (a_j \in M)$$

(すなわち、$a_1 = -T_{L/M}(\alpha), a_e = (-1)^e N_{L/M}(\alpha)$ である) とする。すると、

$$\begin{array}{lcll} \alpha(u_i\alpha^j) & = & u_i\alpha^{j+1} & \text{if } 0 \le j \le e-2 \\ \alpha(u_i\alpha^{e-1}) & = & \sum l = 0^{e-1} \ - a_{e-l}u_i\alpha_l & \text{if } j = e-1 \end{array}$$

となるので、

$$B_\alpha = \begin{pmatrix} 0 & E_d & & & \\ & 0 & E_d & & \\ & & \ddots & \ddots & \\ & & & 0 & E_d \\ -A_{a_e} & -A_{a_{e-1}} & \cdots & -A_{a_2} & -A_{a_1} \end{pmatrix}$$

となる。したがって、

$$T_{L/K}(\alpha) = \mathrm{trace}(B_\alpha) = -\mathrm{trace}(A_{a_1}) = -T_{M/K}(a_1) = T_{M/K}(T_{L/M}(\alpha))$$
$$N_{L/K}(\alpha) = \det(B_\alpha) == (-1)^{d(e-1)}\det(-A_{a_e}) = (-1)^{de}N_{M/K}(a_e) = N_{M/K}(N_{L/M}(\alpha))$$

となる。

$L \supsetneq M(\alpha)$ のときは、命題 33 (2) の証明における行列表示と前半部分を組み合わせればよい。□

命題 35.

K を体、$\overline{K}$ を K の代数閉包とする。L/K を有限次分離拡大とし、$\sigma_1, \cdots, \sigma_d : L \to \overline{K}$ を K 埋め込みとする。このとき、次が成り立つ。

$$\varphi_{\alpha,L/K}(x) = (x - \sigma_1(\alpha))(x - \sigma_1(\alpha)) \cdots (x - \sigma_d(\alpha))$$
$$T_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_d(\alpha)$$
$$N_{L/K} = \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_d(\alpha)$$

$\because$ $L = K(\alpha)$ のときは、α の K 上の最小多項式 $p_{\alpha,K}(x)$ が、$\overline{K}[x]$ の中で

$$p_{\alpha,K}(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_d(\alpha))$$

と 1 次式の積に分解することによる。$L = K(\alpha)$ のときは、命題 33(2) を用いよ。 □

次の定理は、分離性のトレース射による判定法である。標数が 0 のときは、2 つの条件は明らかに成り立つ。

定理 36.

L/K を有限次体拡大とする。このとき、以下は同値である。

(i) L/K は分離拡大である。

(ii) トレース $T_{L/K}$ は零写像でない。

$\because$ (i) $\Rightarrow$ (ii) は次の補題と命題 35 からわかる。

(ii) $\Rightarrow$ (i) : 命題 30 と命題 34 から、非自明な有限次純非分離拡大のときにトレース射は零写像になることを示せばよい。K の標数を $p>0$ とする。命題 29 から L/K の拡大次数が p の倍数だから、$\alpha \in L$ については $T_{L/K}(\alpha)=[L:K]\alpha=0$ となる。$\alpha \notin K$ については、命題 28 から α の K 上の最小多項式が $x^{p^f}-\alpha^{p^f}$ $(f \geq 1)$ となるから、命題 33 から $T_{L/K}(\alpha)=0$ となる。 $\square$

補題 37.

L/K を有限次分離拡大、$\overline{K}$ を K の代数閉包、$\sigma_1, \cdots, \sigma_d\,(d=[L:K])$ を L の $\overline{K}$ の中への K 埋め込みとする。$a_1, \cdots, a_d \in \overline{K}$ に対して、$a_1\sigma_1+\cdots+a_d\sigma_d$ が L 上恒等的に 0 ならば、$a_1=\cdots=a_d=0$ である。

系 38.

L/K を有限次分離拡大とする。このとき、

$$(\ ,\ ): L\times L \to K \quad (\alpha,\beta)\mapsto T_{L/K}(\alpha\beta)$$

は、非退化 K 双線形対称形式である。すなわち、

(i) $(\alpha_1+\alpha_2,\beta)=(\alpha_1,\beta)+(\alpha_2,\beta), (\alpha,\beta_1+\beta_2)=(\alpha,\beta_1)+(\alpha,\beta_2)$.
(ii) $(a\alpha,\beta)=(\alpha,a\beta)=a(\alpha,\beta)$ $(a\in K)$
(iii) $(\alpha,\beta)=(\beta,\alpha)$
(iv) $(\alpha,\beta)=0$ $(\forall\,\beta\in L)$ ならば $\alpha=0$ かつ $(\alpha,\beta)=0$ $(\forall\,\alpha\in L)$ ならば $\beta=0$.

が成り立つ。

3.3. **有限体の Galois 理論.** 有限体について復習する。

定義 39.

有限集合からなる体を**有限体**という。特に、元の数が q 個の体を q 元体という。

素数 p に対して、$\mathbb{F}_p=\mathbb{Z}/(p)$ は p 元体である。

命題 40.

K を有限体とすると、その標数は素数になる。特に、p 元体 $\mathbb{F}_p$ を含む。標数を p とすると、K の元の個数は p の正の整数べきになる。

命題 26 から次が解る。

定理 41.

K を q 元体とすると、K の乗法群は位数が $q-1$ の巡回群である。

定理 42.

p を素数、$\overline{\mathbb{F}}_p$ を $\mathbb{F}_p$ の代数閉包とする。任意の p の正の整数べき q に対して、

$$K=\{\alpha\in\overline{F}_p \,|\, \alpha^q=\alpha\}$$

は、q 元体となる。さらに、$\overline{\mathbb{F}}_p$ に含まれる q 元体は K のみである。

$\because$ K が体になることは、下の補題からわかる。唯一性は、q 元体の乗法群は巡回群なので、各元は方程式 $x^q=x$ の解になる。 $\square$

補題 43.

p を素数、R を 1 の p 個の和が 0 になる環とする。写像

$$\varphi : R \to R \quad \varphi(\alpha) = \alpha^p$$

は、環の準同型になる。特に、R が標数 p の体のとき φ は同型になる。φ のことを Frobenius 射という。

系 44.

p を素数、 q を p の正の整数べきとする。q 元体は同型を除いて一意的である。

$\because$ 代数閉包の間の同型が、q 元体の同型を与える。 □

系 45.

k を有限体、n を正の整数とすると、k の n 次拡大体が存在する。n 次拡大体は k 同型を除いてただ一つ定まる。

系 46.

任意の有限体の拡大は Galois 拡大である。

$\because$ q 元体の各元は分離的多項式 $x^q - x$ の最小分解体になるから。 □

定理 47.

K を q 元体、L を K の r 次拡大、$\varphi_q : L \to L$ を $\varphi(\alpha) = \alpha^q$ (q 乗 Frobenius) とする。このとき、写像

$$\mathbb{Z}/(r) \to \mathrm{Gal}(L/K) \quad a \mapsto \varphi_q^a$$

は群の同型を与える。さらに、M を L の s 次拡大体とするとき

$$\begin{array}{ccccc} \mathrm{Gal}(M/L) & \subset & \mathrm{Gal}(M/K) & \to & \mathrm{Gal}(L/K) \\ \cong\downarrow & & \cong\downarrow & & \downarrow\cong \\ \mathbb{Z}/(s) & \underset{b\mapsto rb}{\longrightarrow} & \mathbb{Z}/(rs) & \underset{\text{自然な射影}}{\longrightarrow} & \mathbb{Z}/(r) \end{array}$$

は可換になる。

$\because$ 補題 43 と定理 42 から、φ_q は L の K 同型になる。L は q^r 元体より、φ_q^r は L 上の恒等写像である。よって、$\varphi_q^a \neq \mathrm{id}_L\,(1 \leq a < r)$ を示せばよい。φ_q^a は q^a 乗写像であり、L の乗法群は位数 $q^r - 1$ の巡回群より、φ_q^a は恒等写像にならない。

後半は、q 乗 Frobenius 写像 φ_q と q^r 乗 Frobenius 写像 φ_{q^r} の行き先を見ればわかる。 □

4. 整拡大

4.1. **整拡大.** 整拡大の一般論を展開する。

命題 48.

B/A を整域の拡大とする。$\alpha \in B$ に対して、以下の命題は同値である。
(i) α は A 上整である。
(ii) B に含まれる自明でない有限生成 A 加群 M が存在して、$\alpha M \subset M$ となる。

補題 49.

B/A を整域の拡大とし、$\alpha \in B$ を A 上整な元とする。このとき、$A[\alpha]$ は A 加群として有限生成である。

$\because$ $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0\,(a_i \in R)$ とする。$A[\alpha]$ は B に含まれる A 加群で、$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ で生成されるものなので、有限生成である。 □

$\because$ 命題 48 の証明 : (i) $\Rightarrow$ (ii) は補題 49.
(ii) $\Rightarrow$ (i) : M の A 上の生成元を $e_1, \cdots, e_n$ とする。仮定より

$$\alpha e_j = a_{1j}e_1 + \cdots + a_{nj}e_n \quad (a_{ij} \in R)$$

と表される。$U = (a_{ij})$ とおき、E_n で n 次の単位行列を表す。$\alpha E_n - U$ は $(e_1, \cdots, e_n)$ を固有値 0 の固有ベクトルとするので、$\det(\alpha E_n - U) = 0$ となる。これを、α に関して展開すると、U の固有多項式が (i) を満たす単多項式を与え得る。 □

注意. 通常、A が体のとき、A 上整な元を単に**代数的**という。

定義から次の命題がすぐにわかる。

命題 50.

A を整域、K を A の商体、$\overline{K}$ を K の代数閉包とする。$\alpha \in \overline{K}$ が A 上整ならば、α の共役元も A 上整である。

定義 51.

B/A を整域の拡大とする。B の元がすべて A 上整のとき、B を A の**整拡大**という。

系 52.

B/A を整域の拡大とし、$\alpha_1, \cdots, \alpha_n \in B$ を B 上整な元とする。このとき、$A[\alpha_1, \cdots, \alpha_r]$ は A 加群として有限生成で、$A[\alpha_1, \cdots, \alpha_r]/A$ は整拡大である。

命題 53.

$C/B/A$ を整域の拡大列とする。
(1) B が A 上の整拡大、$\alpha \in C$ が B 上整とすると、α は A 上整である。
(2) 次は同値である。
(i) C が A の整拡大である。
(ii) B が A の整拡大かつ C が B の整拡大である。

∵ (1) $\alpha^n + b_1\alpha^{n-1} + \cdots + b_n = 0$ とする。系 52 から $D = A[a_1, \cdots, a_n]$ は S に含まれる有限生成である。$M = D + \alpha D + \cdots + \alpha^{n-1}D$ は有限生成 A 加群で C に含まれる。作り方から、$\alpha M \subset M$ である。したがって、α は A 上整である。
(2) は容易。 □

命題 54.

B/A を整拡大とする。
(1) $\mathfrak{q}$ を B の素イデアルとし、A の素イデアルを $\mathfrak{p} = A \cap \mathfrak{q}$ と定める。すると、$B/\mathfrak{q}$ は $A/\mathfrak{p}$ 上の整拡大である。
(2) S を A の積閉集合とする。このとき、$S^{-1}B$ は $S^{-1}A$ 上整拡大である。
(3) B 上の多項式環 $B[x]$ は A 上の多項式環 $A[x]$ 上整拡大である。

∵ (1) $a \in B$　に対して、$\overline{a}$ で $B \to B/\mathfrak{q}$ とする。A に対しても同様。$\overline{\alpha} \in B/\mathfrak{q}$ とすると、α は A の単多項式の零点になるから、それを $\mathfrak{p}$ を法として考えればよい。
(2) $a \in S^{-1}B$ とする。$a = b/s\,(b \in A, s \in S)$ と表せる。$A[b]$ は A 上の有限性成加群だから、$S^{-1}A[a]$ は $S^{-1}A$ 上の有限生成加群である。
(3) $f = b_0 + b_1x + \cdots + b_nx^n \in B[x]\,(b_i \in B)$ とする。$A[b_0, \cdots, b_n]$ は A 上の有限生成加群だから、$A[b_0, \cdots, b_n][x]$ は $A[x]$ 上の有限生成加群になる。 □

4.2. **整閉包.** 整閉包の性質を述べ、代数体の整数環が Noether 整閉整域であることを証明する。

命題-定義 55.

C/A を整域の拡大とする。B を C に含まれる A 上整な元全体とすると、B は C の部分環になり、A 上の整拡大になる。B を A の C の中での**整閉包**という。

∵ B が環になること、すなわち、C の加法と乗法に関して閉じていることを示せばよい。$\alpha, \beta \in C$ を A 上整な元とする。L, M を C に含まれる有限生成 A 加群で、それぞれ $\alpha L \subset L$ かつ $\beta M \subset M$ を満たすとする。$N = LM = \{ab \,|\, a \in L, b \in M\}$ とおくと、N は C に含まれる有限生成 A 加群で $(\alpha + \beta)N \subset N, \alpha\beta N \subset N$ となる。 □

命題 56.

A を整域、K を A の商体、L を K の拡大体とし、B を A の L の中での整閉包とする。
(1) K 上代数的な $\alpha \in L$ に対して、ある $a \in K\,(a \neq 0)$ が存在して $a\alpha \in B$ となる。
(2) B は整閉整域である。
(3) A を整閉整域とすると、$B \cap K = A$ である。

∵ (1) $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0\,(a_i \in K)$ とする。K は A の商体なので、ある $a \in K\,(a \neq 0)$ が存在して、$aa_i \in A\,(\forall i)$ とできる。$(a\alpha)^n + aa_1(a\alpha)^{n-1} + \cdots + a^na_n = 0$　なので、$a\alpha \in B$ である。
(2) B の L の中での整閉包を C とする。$C = B$ を示せばよい。B/A と C/B はともに整拡大なので、C/A も整拡大である。C の定義から $C \subset B$ となる。
(3) は明らか。 □

命題 57.

A を整閉整域、K を A の商体、L を K の有限次拡大とする。$\alpha \in L$ が A 上整ならば、α の特性多項式 $\varphi_{\alpha, L/K}(x)$ は A 係数の多項式である。特に、α のトレース $T_{L/K}(\alpha)$ とノルム $N_{L/K}(\alpha)$ は A に属する。

以下の定理で必要な場合である L/K が分離拡大のときのみ証明する。

∵ 命題 33 より、特性多項式 $\varphi_{\alpha,L/K}(x)$ について証明すればよい。さらに、$L=K(\alpha)$ のとき証明すればよい。命題 35 と命題 50 から、K 上の多項式 $\varphi_{\alpha,L/K}(x)$ の係数は R 上整である。R は整閉より、$\varphi_{\alpha,L/K}(x)$ は R 上の多項式である。 □

定理 58.

B を Noether 整閉整域、K をその商体とする。L を K の有限次分離拡大、A を L の中での R の整閉包とする。このとき、B は Noether 整域である。

∵ $T_{L/K}:L\to K$ を有限次拡大 L/K のトレース写像とする。L/K が分離拡大なので、$T_{L/K}$ は零写像でない。$e_1,\cdots,e_d(d=[L:K])$ を B に含まれる L の K 上の基底とし、N を A 上 $e_1,\cdots,e_d$ で生成される L の部分加群とする。このような基底は、命題 56 から存在する。さて、L の A 部分加群 X に対して、

$$X^*=\{\alpha\in L\,|\,T_{L/K}(\alpha X)\subset A\}]$$

と定める。X^* は A 加群である。系 38 から、N^* は双 1 次形式に関する $e_1,\cdots,e_d$ の双対基底で生成される A 上階数 d の自由加群になる。命題 57 から、$B\subset B^*$ なので、

$$N\subset B\subset B^*\subset N^*$$

となる。A は Noether 環なので、B は有限生成 A 加群になる。したがって、系 21 から B は Noether 整域である。 □

上の 3 つの主張と命題 25 から、次が成り立つ。

定理 59.

代数体 K の整数環 $\mathcal{O}_K$ は Noether 整閉整域である。さらに、$\mathcal{O}_K$ は $\mathbb{Z}$ 上の階数 $[K:\mathbb{Q}]$ の自由加群である。

注. 定理 58 において、A が体上有限生成な環の場合には、L/K が分離的でなくとも B は A 加群として有限生成になる。特に、代数関数体の整数環、すなわち、$k(x)$ (k は体) の有限次拡大における $k[x]$ の整閉包は、$k[x]$ 上有限生成加群で、Noether 整閉整域になる。

4.3. **整拡大と素イデアル.** 代数体の整数環が Dedekind 環であることの証明を完成させる。

定義 60.

B/A を整域の拡大、$\mathfrak{p}$ を A の素イデアルとする。B の素イデアル $\mathfrak{q}$ が $\mathfrak{p}$ の**上にある**とは $\mathfrak{p}=\mathfrak{q}\cap A$ が成り立つことをいう。これを、$\mathfrak{q}\,|\,\mathfrak{p}$ と表す。

定理 61.

B/A を整域の整拡大、$\mathfrak{p}$ を A の素イデアルとする。

(1) B の素イデアル $\mathfrak{q}$ で、$\mathfrak{q}\,|\,\mathfrak{p}$ となるものが存在する。
(2) $\mathfrak{q}\subset\mathfrak{q}'$ を $\mathfrak{p}$ の上にある B の 2 つの素イデアルとすると、$\mathfrak{q}=\mathfrak{q}'$ となる。

補題 62.

B/A を整域の整拡大とする。このとき、「A が体 $\Leftrightarrow$ B が体」が成り立つ。

∵ $\Rightarrow$: $\alpha\in B\,(\alpha\neq 0)$ の B の商体の中での逆元 α^{-1} が B に含まれることを示せばよい。$\alpha^n+a_1\alpha^{n-1}+\cdots+a_n=0\,(a_i\in A)$ とする。B の商体の中で $\alpha^{-1}=-a^{-1}(\alpha^{n-1}+a_1\alpha^{n-2}+\cdots+a_{n-1})$ が成り立つ。A が体なので、α^{-1} は B に含まれる。

$\Leftarrow$: $\alpha \in A\,(\alpha \neq 0)$ の B の中での逆元 α^{-1} が A に含まれることを示せばよい。$\alpha^{-n} + a_1\alpha^{-n+1} + \cdots + a_n = 0\,(a_i \in A)$ とすると、α^{n-1} を掛けると $\alpha^{-1} = -(a_1 + \cdots + a_n\alpha^{n-1})$ となるので、$\alpha^{-1} \in A$ である。 □

$\because$ 定理 61 の証明 : (1) $T = A\backslash\mathfrak{p}$ とし、$B_\mathfrak{p} = T^{-1}A$ と表す。命題 54 (2) から、$B_\mathfrak{p}/A_\mathfrak{p}$ は整拡大である。このとき、$\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$ である。実際、$\mathfrak{p}B_\mathfrak{p} = B_\mathfrak{p}$ とすると、$a_1x_1 + \cdots + a_nx_n = 1\,(a_i \in B_\mathfrak{p}, x_i \in \mathfrak{p}$ となる。したがって、

$$\mathfrak{p}A_\mathfrak{p}[a_1, \cdots, a_n] = A_\mathfrak{p}[a_1, \cdots, a_n]$$

となる。$A_\mathfrak{p}[a_1, \cdots, a_n]$ は有限生成 $A_\mathfrak{p}$ 加群で、$\mathfrak{p}A_\mathfrak{p}$ は $A_\mathfrak{p}$ の唯一の極大イデアルなので、中山の補題から $A_\mathfrak{p}[a_1, \cdots, a_n] = 0$ となってしまう。これは矛盾である。

$\tilde{\mathfrak{q}}$ を $\mathfrak{p}B_\mathfrak{p}$ を含む $B_\mathfrak{p}$ の極大イデアルとし、$\mathfrak{q} = \tilde{\mathfrak{q}} \cap B$ とする。このとき、$\mathfrak{p}A_\mathfrak{p}$ の極大性より、$\tilde{\mathfrak{q}} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ となる。したがって、

$$\mathfrak{q} \cap A = \tilde{\mathfrak{q}} \cap B \cap A = \tilde{\mathfrak{q}} \cap A_\mathfrak{p} \cap A = \mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{p}$$

となる。

(2) 命題 54 (2) と命題 14 から、A は $\mathfrak{q}$ をただ一つの極大イデアルにもつ局所環としてよい。命題 54 (1) から、拡大 $(B/\mathfrak{q})/(A/\mathfrak{p})$ を考えることにより、$\mathfrak{p}$ と $\mathfrak{q}$ はともに零イデアルとしてよい。$A_\mathfrak{p}$ は体なので、補題 62 から $B_\mathfrak{p}$ も体になる。したがって、$\mathfrak{q}' = \mathfrak{q} = (0)$ である。 □

系 63.

B/A を整域の整拡大とする。$\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ を A の素イデアル列とする。このとき、B の素イデアル列 $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \cdots \subsetneq \mathfrak{q}_r$ で、各 i に対して $\mathfrak{q}_i \,|\, \mathfrak{p}_i$ となるものが存在する。

系 64.

A を Dedekind 環、K をその商体とする。L を K の有限次拡大、B を L の中での A の整閉包とする。このとき、仮定 (F)

(F) : B は A 加群として有限生成である。

が成り立つと仮定すると、B は Dedekind 環である。

定理 59 と $\mathbb{Z}$ が P.I.D. であることから、1.1 節の定理 5 が証明できた。

系 65.

代数体の整数環は Dedekind 環である。

注. 前節の注より、代数関数体 K の整数環は、Dedekind 環になる。

5. Dedekind 環

Dedekind 環の分数イデアル全体が乗法に関して群をなし、素イデアル分解の一意性が成り立つことを証明する。

5.1. **分数イデアル.** R を整域、K を R の商体とする。

定義 66.

K に含まれる有限生成 R 加群で、零加群でないものを R の分数イデアルという。

次の 2 つの命題は容易。

命題 67.

(1) I を R の分数イデアルすると、ある $a \in R \setminus \{0\}$ が存在して、aI は R のイデアルになる。
(2) R を Noether 整域とする。K に含まれる R 部分加群 J で、ある $b \in R \setminus \{0\}$ が存在して、bI が R のイデアルならば、J は分数イデアルである。

命題 68.

(1) R の分数イデアル $\mathfrak{a}, \mathfrak{b}$ に対して、
$$\mathfrak{ab} = \left\{ \sum_i x_i y_j \;\middle|\; x_i, \in \mathfrak{a}, y_j \in \mathfrak{b} \right\}$$
と定めると、$\mathfrak{ab}$ は分数イデアルになる。
(2) R の分数イデアル全体 I_R は、上で定めた乗法に関して単位イデアル R を単位元とするモノイドになる。
(3) 分数イデアル $\mathfrak{a}$ が可逆ならば、
$$\mathfrak{a}^{-1} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset R\}$$
となる。(R が Noether ならば右辺の集合はいつでも分数イデアルである。) 特に、単元生成の分数イデアルは可逆である。

分数イデアルの乗法は、通常のイデアルの乗法を分数イデアルに拡張したものになっている。

$\because$ (1) (2) は容易。
(3) 右辺を $\mathfrak{a}^*$ とおく。$\mathfrak{a}^{-1}\mathfrak{a} = R$ より、$\mathfrak{a}^{-1} \subset \mathfrak{a}^*$ となる。$\mathfrak{a}^*\mathfrak{a} \subset R$ より、$\mathfrak{a}^* = \mathfrak{a}^*\mathfrak{a}\mathfrak{a}^{-1} \subset R\mathfrak{a}^{-1} = \mathfrak{a}^{-1}$ である。 □

K に対してその「整数環」が何か一意的に定まるとき、I_R を I_K と表すこともある。

命題 69.

B/A を整域の拡大とする。
$$I_A \to I_B \qquad \mathfrak{a} \mapsto \mathfrak{a}B$$
は、モノイドの準同型を与える。特に、B が A の局所化のとき、全射準同型になる。また、C/B が整域の拡大のとき、自然な図式
$$\begin{array}{ccc} I_A & \to & I_B \\ & \searrow \quad \swarrow & \\ & I_C & \end{array}$$
は可換である。

$\because$ 準同型になることは容易。特に以下の全射性は、A と A の局所化 B の商体が同じであることから解る。 □

5.2. 分数イデアル群.

定理 70.

R を Dedekind 環とする。R の分数イデアル全体 I_R は群になる。また、I_R は R の素イデアル全体を生成元とする自由アーベル群になる。特に、R の零イデアルでないイデアル $\mathfrak{a}$ (単位イデアル R も含む) に対して、素イデアル $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \mathfrak{p}_r$ と正整数 $e_1, \cdots, e_r$ が、$\mathfrak{p}_1, \mathfrak{p}_2, \cdots \mathfrak{p}_r$ の順番を除いて一意的に定まり

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$$

となる。

I_R を R の**イデアル群**という。Dedekind 環の分数イデアルは**素イデアル分解**を一意的に持つことが解る。これは、U.F.D. における素元一意分解の自然な拡張になっている。

定理の証明のために、補題を 2 つ用意する。

補題 71.

R を Noether 環 $\mathfrak{a}$ を任意の零イデアルでないイデアル (単位イデアルも含む) とする。このとき、零イデアルでない素イデアル $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ が存在して、

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{a}$$

となる。

$\because$ Φ を、零イデアルでないイデアルで、素イデアルの積を含まないもの全体の集合とする。Φ が空集合であることが証明できたらよい。Φ を空集合でないとする。R は Noether 環より、Φ には極大元が存在する。Φ の極大元の一つを $\mathfrak{b}$ とする。J は素イデアルでも単位イデアルでもない。よって、$a_1 a_2 \in \mathfrak{b}$ で $a_1, a_2 \notin \mathfrak{b}$ となる R の元 a_1, a_2 が存在する。$\mathfrak{b}_1 = (a_1) + \mathfrak{b}, \mathfrak{b}_2 = (a_2) + \mathfrak{b}$ とする。すると、$\mathfrak{b} \subsetneq \mathfrak{b}_1, \mathfrak{b} \subsetneq \mathfrak{b}_2$ である。$\mathfrak{b}$ の極大性から、$\mathfrak{b}_1, \mathfrak{b}_2 \notin \Phi$ であり、ある素イデアル列、$\mathfrak{q}_{11}, \cdots, \mathfrak{q}_{1s}$ と $\mathfrak{q}_{21}, \cdots, \mathfrak{q}_{2s}$ が存在して、$\mathfrak{q}_{11} \cdots \mathfrak{q}_{1s} \subset \mathfrak{b}_1, \mathfrak{q}_{21} \cdots \mathfrak{q}_{2s} \subset J_2$ となる。よって、

$$\mathfrak{q}_{11} \cdots \mathfrak{q}_{1s} \mathfrak{q}_{21} \cdots \mathfrak{q}_{2s} \subset \mathfrak{b}_1 \mathfrak{b}_2 = \mathfrak{b}^2 + a_1 \mathfrak{b} + a_2 \mathfrak{b} + (a_1 a_2) \subset \mathfrak{b}$$

となり、矛盾が生じた。Φ は空集合である。 □

補題 72.

R を Noether 整域、零イデアルでない R の素イデアルはすべて極大イデアル、K を R の商体とする。零イデアルでない素イデアル $\mathfrak{p}$ に対して

$$\mathfrak{p}^* = \{\alpha \in K \mid \alpha \mathfrak{p} \in R\}$$

とすると、$\mathfrak{p}^* \supsetneq R$ である。

$\because$ $R \subset \mathfrak{p}^*$ は明らか。$\mathfrak{p}^* \neq R$ を示す。$a \in \mathfrak{p} \setminus \{0\}$ をとる。補題 71 より、ある長さが最小の零イデアルでない素イデアル列 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ が存在して、

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$$

となる。素イデアルは極大イデアルより、必要なら順番を取り替えることにより、$\mathfrak{p}_1 = \mathfrak{p}$ とできる。長さの最小性から、

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)$$

となる。$b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ かつ $b \notin (a)$ をとる。$a^{-1} b \notin R$ である。一方、$b\mathfrak{p} \subset (a)$ なので、$a^{-1} b \mathfrak{p} \subset R$ である。すなわち、$a^{-1} b \in \mathfrak{p}^*$ である。したがって、$\mathfrak{p}^* \neq R$ である。 □

$\because$ 定理 70 を証明する。

1° I_R が群になることを証明する。

Φ を零イデアルでないイデアルで、可逆でないもの全体の集合とする。Φ が空集合であることを証明する。Φ が空集合でないとする。R は Noether なので極大元 $\mathfrak{a}$ が存在する。

$\mathfrak{a}$ が素イデアルでないことを証明する。$\mathfrak{a}$ が素イデアルとする。$\mathfrak{a}^*$ を補題 72 の中の記号とする。$\mathfrak{a} \subset \mathfrak{a}^*\mathfrak{a} \subset R$ なので、$\mathfrak{a}$ の極大性から $\mathfrak{a}^*\mathfrak{a}$ は $\mathfrak{a}$ か R のいずれかである。$\mathfrak{a}^*\mathfrak{a} = \mathfrak{a}$ とすると、命題 48 から $\mathfrak{a}^*$ の元はすべて R 上整になり、R の整閉性から $\mathfrak{a}^* \subset R$ となる。これは、補題 72 と矛盾する。

$\mathfrak{a}$ は素イデアルでないことが解った。$\mathfrak{p}$ を $\mathfrak{a}$ を含む素イデアルとする。$\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a} \subset R$ より $\mathfrak{p}^{-1}\mathfrak{a}$ は R のイデアルになる。$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{a}$ とすると、上と同様に $\mathfrak{p}^{-1} \subset R$ となり、補題 72 と矛盾する。$\mathfrak{a}$ の極大性より、 $\mathfrak{p}^{-1}\mathfrak{a}$ は可逆になるので $\mathfrak{a}$ も可逆になり、矛盾が生じた。

以上より、イデアルは可逆であることが解った。

任意の分数イデアルは、単元生成のイデアルをかけるとイデアルになるので可逆である。

2° 任意の零でないイデアルが零イデアルでない素イデアルの積に一意的に表されることを証明する。

積で表されることは、表されないものの集合が空でない都仮定すると、上と同様の議論で矛盾が生じる野で証明できる。一意性を示す。$\mathfrak{a}$ が 2 つの素イデアルの積で表されるとする。すなわち、

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} = \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_t^{t_t}$$

($\mathfrak{p}_i \neq \mathfrak{p}_j\,(i \neq j)$, $\mathfrak{q}$ に着いても同様) とする。両辺に重複する素イデアルをキャンセルすることにより、

$$\mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_s^{e_s'} = \mathfrak{q}_1^{f_1'} \cdots \mathfrak{q}_t^{t_t'}\ (e_i', f_j' \geq 0 \forall i, j)$$

となる。両辺に非自明な素イデアルの積が残るとおかしいので、ちょうどキャンセルできることがわかる。

3° I_R が R の素イデアル全体を生成元とする自由アーベル群になるのは、I_R が R の零イデアルでないイデアル全体がなすモノイドの群化であることと、イデアルが素イデアルによる一意的な分解を持つことから解る。 □

5.3. **近似定理.** R を Dedekind 環、K をその商体、$\mathfrak{p}$ を R の素イデアルとする。$a \in K \setminus \{0\}$ に対して、整数 $v_{\mathfrak{p}}(a)$ を (a) の素イデアル分解における $\mathfrak{p}$ に関するべきで定め、$\mathfrak{p}$ における a の**付値**という。また、$v_{\mathfrak{p}}(0) = \infty$ とする。

補題 73.

$a, b \in K$ に対して、次が成り立つ。

(1) $v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$

(2) $v_{\mathfrak{p}}(a+b) = \inf\{v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)\}$. ただし、$v_{\mathfrak{p}}(a) \neq v_{\mathfrak{p}}(b)$ のとき等号が成り立つ。

∵ (1) 素イデアル分解の一意性より明らか。(2) 命題 69 より、$\mathfrak{p}$ で局所化してよい。すると、$v_{\mathfrak{p}}(a) \geq 0 \Leftrightarrow a \in R_{\mathfrak{p}}$ が成り立つ。$b = 1, a \in R_{\mathfrak{p}}$ の場合を考えればよく、この場合は明らか。 □

定義から次が成り立つ。

命題 74.

R の素イデアル $\mathfrak{p}_1, \cdots \mathfrak{p}_r$ と整数 $e_1, \cdots, e_r$ に対して、

$$\mathfrak{p}^{e_1} \cdots \mathfrak{p}_r^{e_r} = \{\alpha \in K \mid v_{\mathfrak{p}_i}(\alpha) \geq e_i\,(\forall i), v_{\mathfrak{q}}(\alpha) \geq 0\,(\mathfrak{q} \neq \mathfrak{p}_1, \cdots, \mathfrak{p}_r)\}$$

が成り立つ。

定理 75.

R の素イデアル $\mathfrak{p}_1, \cdots \mathfrak{p}_r$、整数 $e_1, \cdots, e_r$ と K の元 $a_1, \cdots, a_r$ に対して、ある K の元 a で

$$v_{\mathfrak{p}_i}(a - a_i) \geq e_i\,(i = 1, \cdots, r),\ v_{\mathfrak{q}}(a) \geq 0\,(\mathfrak{q} \neq \mathfrak{p}_1, \cdots, \mathfrak{p}_r)$$

となるものが存在する。

∵ $c \in R \setminus \{0\}$ を $ca_i \in R\,(\forall i)$ となるようにとる。$\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ でない素イデアルで c を含む素イデアル $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ に対して、それも素イデアルに加え、$f_j = v_{\mathfrak{q}_j}(c), b_j = 0$ とする。そういう素イデアルは有限個であることを注意する。

異なる 2 つの零でない素イデアル $\mathfrak{p}, \mathfrak{q}$ と非負整数 m, n に対して、$\mathfrak{p}^m + \mathfrak{q}^n = R$ とる。実際、$\mathfrak{p} + \mathfrak{q} = R$ の両辺を mn 乗するとよい。中国式剰余定理から、$v_{\mathfrak{p}_i}(a' - ba_i) \geq e_i + v_{\mathfrak{p}_i}(b)\,(\forall i), v_{\mathfrak{q}_j}(a') \geq f_j\,(\forall j)$ となる R の元が存在する。このとき、73 から $a = a'/b$ が求める条件を満たす。 □

系 76.

有限個の極大イデアルしか持たない Dedekind 環は P.I.D. である。

∵ $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ を R の零でない素イデアル全体とする。各 i に対して、$a_{ii} \in \mathfrak{p} \setminus \mathfrak{p}_i^2, a_{ij} = 1\,(j \neq i), e_{ii} = 2, e_{ij} = 1\,(i \neq j)$ ととり、定理 75 を適用して、a_i を得られた K の元とする。すると、$v_{\mathfrak{p}_i}(a_i) = 1, v_{\mathfrak{p}_j}(a_i) = 0\,(j \neq 0)$ となり、$\mathfrak{a}_i = (a_i)$ となる。各素イデアルは単項イデアルであり、イデアルは素イデアルの積で表されるので単項イデアルとなる。したがって、R は P.I.D. である。 □

命題 77.

R を Dedekind 環とし、$\mathfrak{p}$ を零イデアルでない素イデアルとする。任意の非負整数 i に対して、$R/\mathfrak{p}$ ベクトル空間として $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong R/\mathfrak{p}$ となる。。

∵ 命題 15 から R を $\mathfrak{p}$ で局所化してよく、すると R を P.I.D. としてよい。このとき、$\mathfrak{p}$ は単項イデアルである。$\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ をとる。このとき、$R/\mathfrak{p} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}\,(a \mapsto a\pi^i)$ は、$R/\mathfrak{p}$ ベクトル空間としての同型を与える。 □

6. 素イデアルの分解

6.1. **Dedekind 環と素イデアルの分解.** A を Dedekind 環、K をその商体、L を K の有限次拡大体、B を L の中での A の整閉包として、系 64 の仮定 (F)「A 加群として B は有限生成」を満たすとする。B も Dedekind 環になる。

命題 78.

$\mathfrak{p}$ を A の零でない素イデアル、$\mathfrak{q}$ を B の素イデアルとする。このとき次は同値である。

(i) $\mathfrak{q} \mid \mathfrak{p}$.
(ii) $\mathfrak{p}B \subset \mathfrak{q}$.

A の零でない素イデアル $\mathfrak{p}$ に対して、B の素イデアル $\mathfrak{q}_1, \cdots, \mathfrak{q}_g$ を $\mathfrak{q}_i \mid \mathfrak{p}\,(\forall i)$ となるもの全体とする。命題 78 より、$g = g(\mathfrak{p})$ は $\mathfrak{p}$ により決まる正の整数である。B における素イデアル分解

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$$

により、正の整数 $e_i = e(\mathfrak{q}_i/\mathfrak{p})$ を定める。e_i を $\mathfrak{q}_i$ における拡大 B/A の**分岐指数**という。また、$\kappa(\mathfrak{p}) = A/\mathfrak{p}, \kappa(\mathfrak{q}_i) = B/\mathfrak{q}_i$ とおく。B は A 加群として長さ有限より、$\kappa(\mathfrak{q}_i)$ は $\kappa(\mathfrak{p})$ の有限次拡大となる。

$$f_i = f(\mathfrak{q}_i/\mathfrak{p}) = [\kappa(\mathfrak{q}_i) : \kappa(\mathfrak{p})]$$

と定め、$\mathfrak{q}_i$ における**剰余次数**と呼ぶ。

定義 79.

(1) $e_i = 1$ かつ $\kappa(\mathfrak{q}_i)$ が分離拡大のとき、拡大 B/A は $\mathfrak{q}_i$ で**不分岐** という。不分岐でないとき、**分岐**という。$\mathfrak{p}$ の上にあるすべての B の素イデアルで不分岐のとき、拡大 B/A は $\mathfrak{p}$ で不分岐といい、そうでないとき分岐という。
(2) すべての i に対して、$e_i = f_i = 1$ が成り立つとき、拡大 B/A は $\mathfrak{p}$ で**完全分解**するという。
(3) $g = 1$ かつ $f = 1$ のときは、拡大 B/A は $\mathfrak{q}$ で (1 個なので $\mathfrak{p}$ で) **完全分岐**するという。

代数体の整数環の拡大の場合は、剰余体は有限体なので、系 46 からその有限次拡大は分離拡大になる。したがって、不分岐であることと $e(\mathfrak{q}_i/\mathfrak{p}) = 1$ が一致する。

分岐指数、剰余次数には次の関係が成り立つことが定義から容易に解る。

命題 80.

M を L の有限次拡大、C を B の L の中での整閉包とし、条件 (F) を満たすとする。$\mathfrak{p}$ を A の素イデアル、$\mathfrak{q}$ を $\mathfrak{q} \mid \mathfrak{p}$ となる B の素イデアル、$\mathfrak{r}$ を $\mathfrak{r} \mid \mathfrak{q}$ となる C の素イデアルとする。このとき、

$$\begin{aligned} e(\mathfrak{r}/\mathfrak{p}) &= e(\mathfrak{q}/\mathfrak{p})e(\mathfrak{r}/\mathfrak{q}) \\ f(\mathfrak{r}/\mathfrak{p}) &= f(\mathfrak{q}/\mathfrak{p})f(\mathfrak{r}/\mathfrak{q}) \end{aligned}$$

が成り立つ。

分岐指数、剰余次数の間には次の美しい関係が成り立つ。

定理 81.

上の記号の元で、$\displaystyle\sum_{i=1}^{g} e_i f_i = [L : K]$ が成り立つ。

$\because$ $\mathfrak{p}$ で局所化してもよいので、A を初めから局所環としてよい。すると、B の素イデアルは有限個で、系 76 から A と B は P.I.D. である。中国式剰余定理から

$$B/\mathfrak{p}B \cong B/\mathfrak{q}_1^{e_1} \times \cdots \times B/\mathfrak{q}_r^{e_r}$$

となる。両辺は、$\kappa(\mathfrak{p}) = A/\mathfrak{p}$ ベクトル空間になるので、その次元を比べる。命題 25 と命題 56 から、B は自由 A 加群でその階数は $[L : K]$ になる。したって、左辺の次元は $[L : K]$ である。命

題 77 から、$\mathfrak{q}_i^j/\mathfrak{q}_i^{j+1}$ は $\kappa(\mathfrak{q}_i)$ ベクトル空間として 1 次元である。よって、

$$\dim_{\kappa(\mathfrak{p})} B/\mathfrak{q}_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_{\kappa(\mathfrak{p})} \mathfrak{q}_i^j/\mathfrak{q}_i^{j+1} = e_i f_i$$

となる。したがって、求める等式をが証明できた。 □

6.2. **Galois の場合.** A, B, K, L は 6.1 節の状況で、L/K を Galois 拡大とし、その Galois 群を G とする。命題 50 から A 上整な元の共役は A 上整より、G は B に作用する。

命題 82.

$\mathfrak{p}$ を A の零でない素イデアル、$\mathfrak{q}$ を $\mathfrak{q}\,|\,\mathfrak{p}$ となる B の素イデアルとする。$\sigma \in G$ に対して、

$$\sigma(\mathfrak{q}) = \{\sigma(\alpha)\,|\,\alpha \in \mathfrak{q}\}$$

とすると、$\sigma(\mathfrak{q})$ は $\sigma(\mathfrak{q})\,|\,\mathfrak{p}$ となる B の素イデアルである。この対応により、 $\mathfrak{p}$ の上にある B の素イデアルの集合に G が作用し、この作用は推移的である。

∵ 他の部分は容易なので、作用が推移的になることのみ証明する。

推移的でないとして、矛盾を導く。$\mathfrak{r}$ を $\mathfrak{p}$ の上にある B の素イデアルで、G の作用による $\mathfrak{q}$ の軌道に属しないものとする。$\mathfrak{r} + \sigma(\mathfrak{q}) = B\,(\forall \sigma \in G)$ かつ $\sigma(\mathfrak{q}) + \tau(\mathfrak{q}) = B\,(\sigma(\mathfrak{q}) \neq \tau(\mathfrak{q}))$ なので、中国式剰余定理から、ある $x \in B$ で、$x \in \mathfrak{r}$ かつ $x - 1 \in \sigma(\mathfrak{q})\,(\forall \sigma \in G)$ となるものが存在する。命題 35 と命題 57 から、

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{r} \cap A = \mathfrak{p}$$

である。一方、$x \notin \sigma(\mathfrak{q})\,(\forall \sigma \in G)$ なので、$\sigma(x) \notin \mathfrak{q}$ となる。これは、$N_{L/K}(x) \notin \mathfrak{q} \cap A = \mathfrak{p}$ を意味する。 □

系 83.

$\mathfrak{q}$ と $\mathfrak{q}'$ を $\mathfrak{p}$ の上にある B の素イデアルとする。このとき、A 代数として、$B_{\mathfrak{q}}$ と $B_{\mathfrak{q}'}$ は同型になる。特に、分岐指数 $e(\mathfrak{q}/\mathfrak{p})$ と剰余次数 $f(\mathfrak{q}/\mathfrak{p})$ は、$\mathfrak{p}$ の上にある素イデアルの取り方によらず、$\mathfrak{p}$ のみによる。

$\mathfrak{p}$ を A の零でない素イデアル、$\mathfrak{q}$ を $\mathfrak{q}\,|\,\mathfrak{p}$ となる B の素イデアルとする。G の部分群 $D_{\mathfrak{q}}$ を

$$D_{\mathfrak{q}} = \{\sigma \in G\,|\,\sigma(\mathfrak{q}) = \mathfrak{q}\}$$

と定める。$D_{\mathfrak{q}}$ を $\mathfrak{q}$ における**分解群**という。$D_{\mathfrak{q}}$ の固定部分体を $\mathfrak{q}$ での分解体といい、L^d と表す。

$\mathfrak{q}'$ を $\mathfrak{q}'\,|\,\mathfrak{p}$ となる B の素イデアルとし、$\tau \in G$ に対して $\mathfrak{q}' = \tau(\mathfrak{q})$ とする。このとき、

$$D_{\mathfrak{q}'} = \tau D_{\mathfrak{q}} \tau^{-1}$$

となり、分解群は互いに共役である。

命題 84.

上の状況で、$\kappa(\mathfrak{q})$ は $\kappa(\mathfrak{p})$ 上正規拡大で、$D_{\mathfrak{q}}$ は $\kappa(\mathfrak{p})$ 上 $\kappa(\mathfrak{q})$ に作用する。さらに、この作用により誘導される準同型

$$D_{\mathfrak{q}} \to \mathrm{Aut}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$$

は全射である。

$D_{\mathfrak{q}} \to \mathrm{Aut}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ の核を $\mathfrak{q}$ における**惰性群**といい、$I_{\mathfrak{q}}$ と表す。

代数体の整数環の場合は、剰余拡大 $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ は Galois 拡大になる。

∵ $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ が正規拡大であることを証明する。$\alpha \in B$ とし、$\overline{\alpha}$ を α の $\kappa(\mathfrak{q})$ での像とする。$\kappa(\mathfrak{q})$ の $\kappa(\mathfrak{p})$ 上の共役がすべて $\kappa(\mathfrak{q})$ に属することを証明すればよい。$p_{\alpha,K}(x)$ を α の K 上の最小多項式とする。α は A 上整なので、$p_{\alpha,K}(x)$ は A 上の多項式である。$p_{\alpha,K}(x)$ の各係数の $\kappa(\mathfrak{p})$ での像を考えた多項式 $\overline{p}_{\alpha,K}(x)$ は $\overline{\alpha}$ を根に持つ。一方、L/K は Galois 拡大なので、$p_{\alpha,K}(x)$ の根はすべて L に属する。α は A 上整なので、共役元は B に属する。共役元の $\kappa(\mathfrak{q})$ での像を考えると、$\overline{p}_{\alpha,K}(x)$ のすべての根は $\kappa(\mathfrak{q})$ に属する。

$D_{\mathfrak{q}} \to \mathrm{Aut}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ の全射性を証明する。K を分解体 L^d と取り替えることにより、$\mathfrak{p}$ の上にある素イデアルはただ一つとしてよい。k を $\kappa(\mathfrak{q})$ に含まれる $\kappa(\mathfrak{p})$ の最大分離拡大とし、$\alpha \in B$ の元により、$k = \kappa(\mathfrak{q})$ となる。上で証明した正規性より、$k/\kappa(\overline{\alpha})$ は Galois 拡大で、$\mathrm{Aut}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ は $\mathrm{Gal}(k/\kappa(\mathfrak{p}))$ の各元の一意的な $\kappa(\mathfrak{q})$ への延長からなる。α を任意の共役元に移す Galois 群の元が存在するから、$\overline{\alpha}$ をその任意の共役元に移す自己同型が存在する。したがって、全射性が証明できた。 □

命題 85.

上の状況で、次の条件は同値である。

(i) $\mathfrak{q}$ は不分岐である。
(ii) 惰性群 $I_{\mathfrak{q}}$ は単位群である。

∵ e, f, g をそれぞれ、分岐指数、剰余次数、$\mathfrak{p}$ の上にあるイデアルの数とする。定理 81 と系 83 から、$efg = [L:K]$ である。

(i) ⇒ (ii) : $\mathfrak{q}$ は不分岐より、剰余拡大 $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ は Galois 拡大である。よって、$\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ の位数は f である。一方、分解群 $D_{\mathfrak{q}}$ の位数は、命題 系 82 の推移性より $[L:K]/g = f$ となる。全射性より、$D_{\mathfrak{q}} \cong \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ となる。

(ii) ⇒ (i) : $I_{\mathfrak{q}} = \{1\}$ より、

$$ef = [L:K]/g = \sharp \mathrm{Aut}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \leq f$$

が成り立つ。特に、不等号が等号になるのは $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ が分離拡大になるときで、またそのときのみである。したがって、$e = 1$ かつ分離性が示せた。 □

6.3. **ノルム.** A, B, K, L は 6.1 節の状況とする。分数イデアル群の間のノルム

$$N_{B/A} : I_B \to I_A$$

を、各 B の零でない素イデアル $\mathfrak{q}$ で、A の素イデアル $\mathfrak{p}$ の上にあるものに対して、$N_{B/A}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})}$ を満たす準同型とする。$I_{\mathfrak{q}}$ は零でない素イデアルで生成される自由群なので、$N_{B/A}$ が定まる。

命題 86.

(1) M を L の有限次拡大体で、C を M の中での B の整閉包で条件 (F) を満たすものとする。このとき、$N_{C/A} = N_{B/A} \circ N_{C/B}$ となる。
(2) S を A の積閉集合とするとき、自然な図式

$$\begin{array}{ccc} I_B & \xrightarrow{N_{B/A}} & I_A \\ \downarrow & & \downarrow \\ I_{S^{-1}B} & \xrightarrow[N_{S^{-1}B/S^{-1}A}]{} & I_{S^{-1}A} \end{array}$$

は可換である。
(3) $\mathfrak{a}$ を A の分数イデアルとすると、$N_{B/A}(\mathfrak{a}B) = \mathfrak{a}^{[L:K]}$ となる。

∵ (1), (2) は命題 69 と命題 80 から容易。(3) は定理 81 を適用して計算すればよい。 □

体のノルム写像との関係は次のようになる。

定理 87.

$\beta \in L \setminus \{0\}$ とすると、$N_{B/A}((\beta)) = (N_{L/K}(\beta))$ である。

$\because$ 命題 30 と命題 86 から、L/K が分離拡大の場合と非自明な純非分離拡大の場合 (中間体に関する仮定 (F) は、全体に関する仮定 (F) から成り立つ) に証明すればよい。分離拡大の場合は、さらに Galois 拡大としてよい。

命題 86 から A を局所化してもよいので、A はただ一つの素イデアル $\mathfrak{p}$ をもつとする。このとき、B は P.I.D. となる。ノルムは準同型より、β は A 上整としてよい。β が B の単元ならば $N_{L/K}(\beta)$ は A の単元になる。よって、β を B の素元、すなわち、ある $\mathfrak{p}$ の上にある素イデアル $\mathfrak{q}$ の生成元としてよい。

1°. L/K が Galois 拡大とし、その Galois 群を G とする。e, f, g を $\mathfrak{p}$ に関する分岐指数、剰余次数、上にある素イデアルの個数とし、$\mathfrak{q}_1, \cdots, \mathfrak{q}_g$ を $\mathfrak{p}$ の上にある素イデアルとする。自然な写像 $I_A \to I_B$ は単射なので、$N_{L/K}(\beta)B = \mathfrak{p}^f B$ を証明すればよい。実際、

$$N_{L/K}(\beta)B = \prod_{\sigma \in G} \sigma(\beta)B = \prod_{\sigma \in G} \sigma(\mathfrak{q}) = \prod_{i=1}^{g} \prod_{\sigma \in D_{\mathfrak{q}_i}} \mathfrak{q}_i = \mathfrak{q}_1^{ef} \cdots \mathfrak{q}_g^{ef} = \mathfrak{p}^f B$$

となる。

2°. K の標数を $p > 0$ とし、L/K が非自明な純非分離拡大とする。L/K を p 次の拡大としてよい。$\beta^p \in K$ より、

$$N_{B/A}(\mathfrak{q})^p = N_{B/A}(\beta^p B) = (N_{L/K}(\beta))^p$$

となる。I_A は自由群より、$N_{B/A}(\mathfrak{q}) = (N_{L/K}(\beta))$ である。 □

さて、K を代数体で、$\mathcal{O}_K$ を K の整数環とする。$\mathfrak{a}$ を $\mathcal{O}_K$ の零でないイデアル (単位イデアルでもよい) とするとき、$\mathcal{O}_K/\mathfrak{a}$ は有限環 (単位イデアルのときは 1 元からなる零環) になる。

$$N : I_K \to \mathbb{Z}$$

を $N(\mathfrak{a}) = \sharp \mathcal{O}_K/\mathfrak{a}$ と定める。

命題 88.

$\mathcal{O}_K$ の零でないイデアル $\mathfrak{a}$ に対して、$N(\mathfrak{a}) = \sharp \mathbb{Z}/N_{\mathcal{O}_K/\mathbb{Z}}(\mathfrak{a})$ となる。特に、$\mathcal{O}_K$ の零でないイデアル $\mathfrak{a}, \mathfrak{b}$ に対して、$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ が成り立つ。

$\because$ $\mathfrak{p}$ を $\mathcal{O}_K$ の零でない素イデアルで、素数 p で生成されるイデアルの上にあるイデアルとすると、

$$\sharp \mathcal{O}_K/\mathfrak{p} = p^{[\kappa(\mathfrak{p}):\mathbb{F}_p]} = \sharp \mathbb{Z}/(p^{[\kappa(\mathfrak{p}):\mathbb{F}_p]})$$

となる。さらに、命題 77 から、任意の正整数 n に対して、

$$\sharp \mathcal{O}_K/\mathfrak{p}^n = \prod_{i=0}^{n} \sharp \mathfrak{p}^i/\mathfrak{p}^{i+1} = (\sharp \mathcal{O}_K/\mathfrak{p})^n$$

となる。素イデアル分解の一意性と中国式剰余定理から、命題は証明できる。 □

7. 単拡大の場合

Dedekind 環の拡大 B/A が単拡大の場合に、素イデアルの分解を考察する。一般には、B が A 上の単拡大にはならないことを注意しておく。

7.1. **分岐する素イデアル.** A を Dedekind 環、K をその商体、L を K の有限次拡大体、B を L の中での A の整閉包とし、系 64 の仮定 (F)「B は A 加群として有限生成である。」が成り立つとする。このとき、B は Dedekind 環である。さらに、B は A 上単元生成、すなわち、ある $\alpha \in B$ が存在して、$B = A[\alpha]$ とする。α の K 上の最小多項式を $p_{\alpha,K}(x)$ とすると、命題 57 から $p_{\alpha,K}(x)$ は A 係数の単多項式である。

$\mathfrak{p}$ を A の零でない素イデアル、$\kappa(\mathfrak{p}) = A/\mathfrak{p}$ とする。A 係数多項式 $f(x)$ に対して、$\overline{f}(x)$ で $f(x)$ の $\kappa(\mathfrak{p})$ での自然な像を表すことにする。

定理 89.

ある A 係数単多項式 $q_1(x), \cdots, q_g(x)$ で $\overline{q}_1(x), \cdots, \overline{q}_g(x)$ が互いに異なる $\kappa(\mathfrak{p})$ 上の既約単多項式により、

$$\overline{p}_{\alpha,K}(x) = \overline{q}_1(x)^{e_1} \cdots \overline{q}_g(x)^{e_g}$$

と既約分解されるとする (いつでもこのような既約分解を持つ)。このとき、

$$\mathfrak{q}_i = \mathfrak{p}B + (q_i(\alpha)) \ (i = 1, \cdots, g)$$

は $\mathfrak{p}$ の上にある B の互いに異なる素イデアルはであり、$\mathfrak{p}$ の上にある素イデアルはこれらのみである。さらに、

$$\begin{aligned} e(\mathfrak{q}_i/\mathfrak{p}) &= e_i \\ f(\mathfrak{q}_i/\mathfrak{p}) &= \deg(q_i(x)) \end{aligned}$$

が成り立つ。

$\because$ $B = A[x]/(p_{\alpha,K}(x))$ より、中国式剰余定理から

$$B/\mathfrak{p}B \cong A[x]/(\mathfrak{p} + (p_{\alpha,K}(x))) \cong \kappa[x]/(\overline{p}_{\alpha,K}(x)) \cong \kappa[x]/(\overline{q}_1(x)^{e_1}) \times \cdots \times \kappa[x]/(\overline{q}_g(x)^{e_g})$$

になる。$(\overline{q}_i(x))$ は $k[x]$ の素イデアルより、準同型

$$B \to \kappa[x]/(\overline{q}_i(x))$$

の逆像が、B の $\mathfrak{p}$ の上にある素イデアルを与える。したがって、$\mathfrak{q}_i = \mathfrak{p}B + (q_i(\alpha)) \, (i = 1, \cdots, g)$ が求める素イデアルであり、分岐指数、剰余次数の対応が成り立つ。 □

系 90.

$p'_{\alpha,K}(\alpha)$ で $p_{\alpha,K}(\alpha)$ の微分を表す。$\mathfrak{D} = (p'_{\alpha,K}(\alpha))$ を B のイデアルとする。$\mathfrak{q}$ を $\mathfrak{q} \mid \mathfrak{p}$ となる B の素イデアルとする。このとき、次は同値である。

(i) 拡大 B/A は $\mathfrak{q}$ で分岐する。
(ii) $\mathfrak{D} \subset \mathfrak{q}$

$\because$ 定理 89 の記号を用いる。$\mathfrak{q} = \mathfrak{q}_1$ とする。

(i) $\Rightarrow$ (ii) の証明 : $\kappa(\mathfrak{q}) = B/\mathfrak{q}$ とおく。$\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ が非分離拡大のとき、$\overline{q}'_1(x) = 0$ となる。$\overline{p}_{\alpha,K}(x) = \overline{q}_1(x)^{e_1} \cdots \overline{q}_g(x)^{e_g}$ なので、$p'_{\alpha,K}(\alpha) \in \mathfrak{p}B + (q_1(\alpha)^{e_1}) \subset \mathfrak{q}$ となる。

$\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ が分離拡大のとき、$e(\mathfrak{q}/\mathfrak{p}) = e_1 > 1$ である。$p'_{\alpha,K}(\alpha) \in \mathfrak{p}B + (q_1(\alpha)^{e_1-1}) \subset \mathfrak{q}$ となる。

(ii) $\Rightarrow$ (i) : $e(\mathfrak{q}/\mathfrak{p}) = e_1 = 1$ とする。逆をたどることにより、$p'_{\alpha,K}(\alpha) \in \mathfrak{q}$ は $q'_1(\alpha) \in \mathfrak{q}$ を意味する。$\overline{q}_1(x)$ は $x = \overline{\alpha}$ を根に持つ既約多項式で、$\overline{q}'_1(\overline{\alpha}) = 0$ より分離的でない。 □

7.2. 2 **次体の場合.** 最初に平方剰余記号を導入する。

p を奇素数 ($p \geq 3$ なる素数ということ) とする。p と素な整数 a に対して、p を法として a が平方数になるとき a は p を法として**平方剰余**といい、そうでないとき**平方非剰余**という。すなわち、

$$a \text{ は平方剰余} \quad \Leftrightarrow \quad a \equiv b^2 \pmod{p} \, (\exists b \in \mathbb{Z})$$

と定める。さらに、

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ただし } a \text{ は平方剰余} \\ -1 & \text{ただし } a \text{ は平方非剰余} \end{cases}$$

と定める。$\{\pm 1\}$ は、適当な体の単数群の部分群に値をとる。$\left(\frac{a}{p}\right)$ を**ルジャンドル記号**という。

命題 91.

$a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. 特に、$\left(\frac{a}{p}\right)$ は $\mathbb{F}_p^\times$ から $\{\pm 1\}$ への写像と見なせる。

a が p で割れるとき、$\left(\frac{a}{p}\right) = 0$ として拡張しておく。

命題 92.

$a \in \mathbb{F}_p^\times$ とする。このとき、次が成り立つ。

$$a^{\frac{p-1}{2}} = 1 \Leftrightarrow \exists b \in \mathbb{F}_p \text{ s.t. } a = b^2$$

特に、$\mathbb{F}_p$ の中で

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

である。これを、**オイラー規準**という。

$\because$ α を $\mathbb{F}_p^\times$ の生成元とし、$a = \alpha^r$ とする。α の位数はちょうど $p-1$ なので、

$$a^{\frac{p-1}{2}} = 1 \Leftrightarrow p-1 \,\Big|\, \frac{p-1}{2} r \Leftrightarrow 2 \,|\, r \Leftrightarrow a = (\alpha^{\frac{r}{2}})^2$$

となる。また、$\mathbb{F}_p^\times$ は位数が $p-1$ なので、$a^{\frac{p-1}{2}} = \pm 1$ である。 □

定理 (Gauss) 93.

(1) と (2) では p を奇素数、(3) では p, q を互いに異なる奇素数とする。

(1) (第 1 補充則) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$

(2) (第 2 補充則) $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8}. \end{cases}$

(3) (平方剰余の相互法則) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

さて、2 次体の整数環における素元の分解を考察する。

D を平方因子を持たない整数とし、$K = \mathbb{Q}(\sqrt{D})$ とする。2 次体における素イデアルの分解を決定する。2 次拡大は Galois 拡大より、命題 83 から素数 p ごとに $\mathbb{Z}$ の素イデアル (p) の上にある素イデアルの分岐指数、剰余次数が決まり、それらを e_p, f_p とする。また、(p) の上にあるイデアルの個数を g_p とすると、定理 81 から $e_p f_p g_p = 2$ となる。したがって、3 つのパターン

$$(e_p, f_p, g_p) = (2,1,1), (1,2,1), (1,1,2)$$

のみ起きうる。それぞれ、素数 p は分岐、惰性的、完全分解するという。

$$D_K = \begin{cases} |D| & \text{if } D \equiv 1 \pmod{4} \\ 4|D| & \text{if } D \equiv 2, 3 \pmod{4} \end{cases}$$

とおき、K の**判別式**という。

定理 94.

(1) p は分岐 $\Leftrightarrow p \mid D_K$

(2) p が惰性的 $\Leftrightarrow \begin{cases} p \text{は奇素数かつ} \left(\dfrac{D}{p}\right) = -1 \\ \text{または} \\ D \equiv 5 \pmod 8 \text{かつ} p = 2 \end{cases}$

(3) p が完全分解 $\Leftrightarrow \begin{cases} p \text{は奇素数かつ} \left(\dfrac{D}{p}\right) = 1 \\ \text{または} \\ D \equiv 1 \pmod 8 \text{かつ} p = 2 \end{cases}$

$\because$ $D \equiv 3 \pmod 4$ のときのみ証明する。定理 9 から $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$ である。$p_{\sqrt{D},\mathbb{Q}}(\sqrt{D}) = x^2 - D$ を、$\sqrt{D}$ の $\mathbb{Q}$ 上の最小多項式とする。分岐する $\mathcal{O}_K$ の素イデアルは、系 90 から $p_{\sqrt{D},\mathbb{Q}}(\sqrt{D}) = 2\sqrt{D}$ を含むことが必要十分条件になる。$N_{\mathcal{O}_K/\mathbb{Z}}(2\sqrt{D}) = (4D) = (D_K)$ なので、分岐する素数 p の必要十分条件は $p \mid D_K$ である。

$p \nmid D_K$ とする。$\overline{p}_{\sqrt{D},\mathbb{Q}}(x)$ を $p_{\sqrt{D},\mathbb{Q}}(x)$ の $\mathbb{F}_p[x]$ での像とする。定理 89 を用いると、p が惰性的であることと $\overline{p}_{\sqrt{D},\mathbb{Q}}(x)$ が 既約であることは同値である。よって、D が p を法として平方非剰余ということが必要十分条件である。 □

7.3. **Galois 拡大でない例.** $K = \mathbb{Q}(2^{\frac{1}{3}})$ とする。$K/\mathbb{Q}$ は Galois 拡大でない。計算をすることにより、K の整数環は

$$\mathcal{O}_K = \mathbb{Z}[2^{\frac{1}{3}}]$$

となり、$2^{\frac{1}{3}}$ の $\mathbb{Q}$ 上の最小多項式は $p_{2^{\frac{1}{3}},\mathbb{Q}}(x) = x^3 - 2$ である。$p'_{2^{\frac{1}{3}},\mathbb{Q}}(2^{\frac{1}{3}}) = 3 \times 2^{\frac{2}{3}}$ より、系 90 から分岐する素イデアルは 2 または 3 の上にのみある。

素数 p に対して $p_{2^{\frac{1}{3}},\mathbb{Q}}(x)$ の $\mathbb{F}_p$ における像 $\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x)$ の既約分解の様子を調べる。

補題 95.

(1) $p = 2$ とすると、$\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x) = x^3$ となる。

(2) $p = 3$ とすると、$\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x) = (x-2)^3$ となる。

(3) $p \neq 2, 3$ とすると、$\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x)$ は分離的である。さらに次が成り立つ。

  (i) $p \equiv 1 \pmod 3$ かつ $\overline{2} \in (\mathbb{F}_p^\times)^3$ ならば $\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x)$ は 3 つの 1 次式の積に既約分解される。

  (ii) $p \equiv 1 \pmod 3$ かつ $\overline{2} \notin (\mathbb{F}_p^\times)^3$ ならば $\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x)$ は 3 次の既約多項式である。

  (iii) $p \equiv 2 \pmod 3$ ならば $\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x)$ は 1 次式 $\times$ 2 次式と既約分解される。

定理 89 と系 90 から、$\mathcal{O}_K$ における素数の分解は次のようになる。

定理 96.

(1) $p = 2$ とすると、(2) の上にある素イデアルは $(2^{\frac{1}{3}})$ ただ 1 つで、$e = 3, f = 1$ である。

(2) $p = 3$ とすると、(3) の上にある素イデアルは $(2^{\frac{1}{3}} - 2)$ ただ 1 つで、$e = 3, f = 1$ である。

(3) $p \neq 2, 3$ とすると、$\overline{p}_{2^{\frac{1}{3}},\mathbb{Q}}(x)$ は分離的である。さらに次が成り立つ。

  (i) $p \equiv 1 \pmod 3$ かつ $\overline{2} \in (\mathbb{F}_p^\times)^3$ ならば (p) の上にある素イデアルは 3 つあり、分岐指数と剰余次数はすべて同じで 1 である。

  (ii) $p \equiv 1 \pmod 3$ かつ $\overline{2} \notin (\mathbb{F}_p^\times)^3$ ならば (p) の上にある素イデアルは $p\mathcal{O}_K$ ただ 1 つで、$e = 1, f = 3$ となる。さらに、既約多項式である。

  (iii) $p \equiv 2 \pmod 3$ ならば (p) の上にある素イデアルは 2 つあり、それぞれ $e = 1, f = 1$ と $e = 1, f = 2$ になる。